

02-07-00

A

## IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventorship..... Maller  
 Applicant..... Microsoft Corporation  
 Attorney's Docket No. .... MS1-353US  
 Title: Email Filtering Methods and Systems

TRANSMITTAL LETTER AND CERTIFICATE OF MAILING

To: Commissioner of Patents and Trademarks  
 Washington, D.C. 20231

From: Lance R. Sadler (509) 324-9256  
 Lee & Hayes, PLLC  
 421 W. Riverside Avenue, Suite 500  
 Spokane, WA 99201

The following enumerated items accompany this transmittal letter and are being submitted for the matter identified in the above caption.

1. Transmittal Letter with Certificate of Mailing included.
2. PTO Return Postcard Receipt
3. Check in the Amount of \$ 1774.00
4. Fee Transmittal
5. New patent application (title page plus 39 pages, including claims 1-52 & Abstract)
6. Executed Declaration
7. 8 sheets of formal drawings (Figs. 1-10)
8. Assignment w/Recordation Cover Sheet

Large Entity Status ☒ [x]

Small Entity Status ☐ [ ]

The Commissioner is hereby authorized to charge payment of fees or credit overpayments to Deposit Account No. 12-0769 in connection with any patent application filing fees under 37 CFR 1.16, and any processing fees under 37 CFR 1.17.

Date: 2/4/00

By: 

Lance R. Sadler  
 Reg. No. 38,605

CERTIFICATE OF MAILING

I hereby certify that the items listed above as enclosed are being deposited with the U.S. Postal Service as either first class mail, or Express Mail if the blank for Express Mail No. is completed below, in an envelope addressed to The Commissioner of Patents and Trademarks, Washington, D.C. 20231, on the below-indicated date. Any Express Mail No. has also been marked on the listed items.

Express Mail No. (if applicable) EL472378773

Date: 2/4/2000

By: 

Dana L. Calhoun

02/04/00  
 jc490 U.S. PTO

jc675 U.S. PTO  
 09/497992  
 02/04/00

09497992 020400

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION FOR LETTERS PATENT

**Email Filtering Methods and Systems**

Inventor(s):  
Steven T. Maller

ATTORNEY'S DOCKET NO. MS1-353US

004020"26646460

1 **TECHNICAL FIELD**

2 This invention relates to email filtering methods and systems.

3  
4 **BACKGROUND OF THE INVENTION**

5 Email systems facilitate the exchange of electronic mail over a network,  
6 such as a LAN (local area network), WAN (wide area network), or public network  
7 (e.g., Internet). Most people are familiar with traditional computer email systems,  
8 which are constructed on a client-server model. The email system involves a  
9 server-based mail program residing on the server computer to manage the  
10 exchange of email messages over one or more networks and a client-based mail  
11 program residing on the client to implement a mailbox that receives and holds the  
12 email messages for a user. The client-based mail program also implements a  
13 graphical user interface that enables the user to open and read mail, or to create  
14 new mail messages.

15 Other email systems have evolved that are more focused on the server side  
16 of the equation than on the client side. In these types of systems, email servers  
17 provide the bulk of the functionality that a client sees when the client enters the  
18 email environment. One such system is shown generally at 20 in Fig. 1 and  
19 includes an email server system 22 having a processor 24 that is configured to  
20 receive email messages from a sender and distribute copies of the email messages  
21 to one or more recipients. A recipient storage location 26 is provided and includes  
22 a plurality of storage locations that are dedicated to individual recipients, with  
23 three exemplary dedicated storage locations being shown at 28, 30 and 32. The  
24 email messages that are received by the server system are copied directly into the  
25 dedicated storage locations (sometimes referred to as "inboxes") for each

1 recipient. If one message is received with nine specified recipients, then nine  
2 copies of the message are made and placed into nine separate dedicated recipient  
3 storage locations.

4 In systems such as these, many of the functions that are traditionally  
5 implemented by a client machine are implemented by the server system 22. For  
6 example, email messages, records, passwords, user preferences, address lists, and  
7 the like are all saved on the server side in storage locations that are dedicated for  
8 each recipient. Recipients or clients must then typically log in with the server and  
9 run a browser program that lets them work within the email system to read their  
10 messages. Logging in with the server is typically accomplished over a computer  
11 network such as the Internet, and through the use of a suitable web browser. The  
12 email environment is generated by the server through the use of HTML or web  
13 pages that present the recipient or client with a screen that looks like an email box.  
14 All email messages are delivered using the web page format. Microsoft's Hotmail  
15 service is an exemplary system.

16 Email is a tremendously fast and efficient way to send electronic messages.  
17 One of the problems that plagues the efficient use of email is the growing presence  
18 of unwanted and unsolicited emails. These emails are typically referred to as  
19 "spam." Spam can include unsolicited commercial emails (UCE) or non-  
20 commercial emails. Spam is a menace that clogs email systems, slows down  
21 performance, and severely impacts the manner in which email services are  
22 provided by an email server to its clients.

23 From an operational standpoint, UCE or spam can consume vast amounts  
24 of disk space and can monopolize many other machine resources. For example, in  
25 the Fig. 1 example, when an email message is received by server system 22, a

1 copy for each intended recipient is made and placed into the dedicated storage  
2 location for each recipient. In the illustrated example, processor 24 receives a  
3 spam message and makes a copy of the spam message for each of the intended  
4 recipients, i.e. recipients 28, 30 and 32. If a large number of recipients are  
5 specified by the sender, then a large amount of server memory can be consumed  
6 by replicating the message and placing it in each dedicated storage location for  
7 each specified recipient. The typical message has the following fields that are  
8 shown in the figure: "TO", "FROM", "CC", "BC", and "SUBJECT".

9 From a customer service standpoint, system administrators are often at a  
10 loss to combat the delivery of spam to their individual clients. This can and often  
11 does result in large numbers of complaints and bounced email messages.  
12 Additionally, customers often do not wish to even receive certain types of morally  
13 or otherwise offensive emails. Yet, because the spammers (those who promulgate  
14 spam) predominate, innocent clients continue to be bombarded with unwanted  
15 email messages. From a legal standpoint, valuable time and resources are wasted  
16 in pursuing spammers because of the various havoc they wreak on network  
17 systems. Needless to say, spam continues to plague those who are in the business  
18 of providing email services to clients.

19 Accordingly, this invention arose out of concerns associated with providing  
20 improved systems and methods for reducing the impact that UCE and spam has on  
21 email recipients.

## 22 SUMMARY OF THE INVENTION

24 Various embodiments of the invention address two critical problems that  
25 current email service providers face. First, there is the problem of maintaining

high levels of customer service when email server systems are inundated with spam. Second, there is the problem of reducing the system-wide impact that spam has on the email delivery system. Current embodiments are directed to determining whether an email message is an unwanted bulk email message without necessarily considering the message that is conveyed by any portion of the email message. Through analyses of patterns of delivery of these email messages, profiles are built that allow an email server to ascertain whether there is a likelihood that any one particular email message constitutes an unwanted email message. If an email message is determined to likely constitute an unwanted email message, then memory-saving measures are implemented. In preferred embodiments, one copy of the email message is saved at a central, shared location that can be accessed by each of the intended recipients. This avoids having to replicate the email message across the system for each of the recipients.

#### **BRIEF DESCRIPTION OF THE DRAWINGS**

Fig. 1 is a high level diagram of a prior art email server system.

Fig. 2 is a flow diagram that describes a process in accordance with one embodiment of the invention.

Fig. 3 is a diagram of a computer system that can be used to implement various embodiments of the invention.

Fig. 4 is a high level diagram of an email server system in accordance with one embodiment of the invention.

Fig. 5 is a diagram of the Fig. 4 email server system.

Fig. 6 is a flow diagram that describes processing in accordance with one embodiment of the invention.

1 Fig. 7 is a diagram of a desirability index in accordance with one  
2 embodiment of the invention.

3 Fig. 8 is a diagram of a user interface in accordance with one embodiment  
4 of the invention.

5 Fig. 9 is a flow diagram that describes processing in accordance with one  
6 embodiment of the invention.

7 Fig. 10 is a diagram of an email delivery system in accordance with a  
8 preferred embodiment of the invention.

## 9 10 **DETAILED DESCRIPTION**

### 11 **Overview**

12 Unwanted email messages can come in many different packages such as  
13 unsolicited commercial email (UCE) messages that seek to have recipients invest  
14 or spend money, or email messages that are not necessarily commercial in nature,  
15 but nonetheless are undesirable because of their message content, e.g. obscene or  
16 morally inflammatory email messages. Various embodiments of the invention  
17 recognize that unwanted emails messages often typically have delivery patterns  
18 that distinguish them from other wanted emails. The delivery patterns are often  
19 independent of the messages conveyed by any of the content of the email  
20 messages, e.g. independent of the content of the sender's address field, the subject  
21 field, and the message field. That is, determining that an email message is  
22 unwanted does not necessarily depend on reading an email message and  
23 interpreting its content. For example, some of the patterns that unwanted email  
24 messages exhibit are that they typically specify a large number of recipient  
25 addresses, and a determinable percentage of the specified recipient addresses may

1 be invalid. Another pattern concerns the size of the email message. That is, many  
2 unwanted email messages are larger than a determinable size. Over time, profiles  
3 are built based upon the these and other delivery patterns. These profiles are then  
4 used by the server to assess an incoming email message and determine whether it  
5 is likely to constitute an unwanted email message. Without reading the content of  
6 an email message it is difficult to ascertain with complete certainty whether it is in  
7 fact unwanted. Yet, the profiles that are built can assign a degree of likelihood that  
8 any given email message does or does not constitute an unwanted email message.

9 If an email message likely constitutes an unwanted email message, then one  
10 or more preventative measures can be taken to minimize the impact that the email  
11 message has on its intended recipients and on the server system. For example, the  
12 server might redirect an incoming email message if it has determined that the  
13 email message is likely to be unwanted. Such redirection might involve, for  
14 instance, placing the email message in a specially-defined "folder" or storage  
15 location, which has been created to receive such messages. As another example  
16 useful in various server-side embodiments, if a server determines that an incoming  
17 email message likely constitutes an unwanted email message, the server makes a  
18 single copy of it and places it in a shared storage location. This shared location is  
19 represented to the user as a special folder or storage location similar to an inbox.  
20 Individual recipients are notified and can read the email message at the shared  
21 location. Thus, the server avoids having to make and store numerous copies of the  
22 email message. If a recipient so desires, they can request a copy of the email  
23 message at which time the server places a copy of it in a dedicated recipient  
24 storage location for them.



1       Embodiments of the invention also provide a robust collection of heuristics  
2 that go far beyond simply screening an email message based upon a sender's  
3 address. The heuristics can consider parameters that are independent of the  
4 message conveyed by any content portion of an email message, and/or parameters  
5 that are dependent upon the message thus conveyed. Flexibility is provided by  
6 enabling the parameters to be adjusted to accommodate different patterns. For  
7 example, one set of heuristics might be used during prime computing time, while  
8 another set is used during slower computing times.

9       Further, solutions are provided that enable the server and its clients to work  
10 in concert to uniquely tailor the server's screening to fit the individual needs of the  
11 clients. The concept of a desirability index establishes values that are assigned to  
12 various degrees of desirability that an email message can have. Various  
13 parameters having parameter values are associated with each index value. A user  
14 can adjust either the parameter values or the index values to establish a degree of  
15 desirability. Email messages are then evaluated against the defined index value.

16       Fig. 2 shows a flow diagram at 100 that describes processing in accordance  
17 with embodiments of the invention. The processing that is described preferably  
18 takes place on the server side and is executed by the server system. The server can  
19 be a dedicated server that is specifically programmed to screen email messages. A  
20 profile of unwanted email is first developed at step 102. The profile preferably  
21 takes into account information that is not dependent upon the message conveyed  
22 by any of the content of an email message. The server is configured at step 104 to  
23 screen email messages based upon the profile. The server evaluates each of the  
24 email messages that it receives at step 106. If an email message meets the profile,  
25 then the server places a copy of the email message in a central location at step 108

1 and sends a notification to each of the recipients that an email message has been  
2 received. In preferred embodiments, only one copy is saved by the server,  
3 although other copies can be made if a recipient has specifically requested to  
4 receive email messages from a particular sender. The one copy is placed in a  
5 location that can be shared by each of the intended recipients for reading the  
6 message. If an email message does not meet the profile, then the server delivers  
7 the email message to a recipient storage location at step 110. In this way, email  
8 messages that have a high likelihood of constituting unwanted email or spam are  
9 not replicated across the server's storage system. Rather, storage is conserved by  
10 saving only one copy of the email message.

### 11 12 **Computer System**

13 Preliminarily, Fig. 3 shows a general example of a desktop computer 130  
14 that can be used in accordance with the invention. Computer 130 can be used to  
15 implement server or client machines.

16 Computer 130 includes one or more processors or processing units 132, a  
17 system memory 134, and a bus 136 that couples various system components  
18 including the system memory 134 to processors 132. The bus 136 represents one  
19 or more of any of several types of bus structures, including a memory bus or  
20 memory controller, a peripheral bus, an accelerated graphics port, and a processor  
21 or local bus using any of a variety of bus architectures. The system memory 134  
22 includes read only memory (ROM) 138 and random access memory (RAM) 140.  
23 A basic input/output system (BIOS) 142, containing the basic routines that help to  
24 transfer information between elements within computer 130, such as during start-  
25 up, is stored in ROM 138.

Computer 130 further includes a hard disk drive 144 for reading from and writing to a hard disk (not shown), a magnetic disk drive 146 for reading from and writing to a removable magnetic disk 148, and an optical disk drive 150 for reading from or writing to a removable optical disk 152 such as a CD ROM or other optical media. The hard disk drive 144, magnetic disk drive 146, and optical disk drive 150 are connected to the bus 136 by an SCSI interface 154 or some other appropriate interface. The drives and their associated computer-readable media provide nonvolatile storage of computer-readable instructions, data structures, program modules and other data for computer 130. Although the exemplary environment described herein employs a hard disk, a removable magnetic disk 148 and a removable optical disk 152, it should be appreciated by those skilled in the art that other types of computer-readable media which can store data that is accessible by a computer, such as magnetic cassettes, flash memory cards, digital video disks, random access memories (RAMs), read only memories (ROMs), and the like, may also be used in the exemplary operating environment.

A number of program modules may be stored on the hard disk 144, magnetic disk 148, optical disk 152, ROM 138, or RAM 140, including an operating system 158, one or more application programs 160, other program modules 162, and program data 164. A user may enter commands and information into computer 130 through input devices such as a keyboard 166 and a pointing device 168. Other input devices (not shown) may include a microphone, joystick, game pad, satellite dish, scanner, or the like. These and other input devices are connected to the processing unit 132 through an interface 170 that is coupled to the bus 136. A monitor 172 or other type of display device is also

1 connected to the bus 136 via an interface, such as a video adapter 174. In addition  
2 to the monitor, personal computers typically include other peripheral output  
3 devices (not shown) such as speakers and printers.

4 Computer 130 commonly operates in a networked environment using  
5 logical connections to one or more remote computers, such as a remote computer  
6 176. The remote computer 176 may be another personal computer, a server, a  
7 router, a network PC, a peer device or other common network node, and typically  
8 includes many or all of the elements described above relative to computer 130,  
9 although only a memory storage device 178 has been illustrated in Fig. 2. The  
10 logical connections depicted in Fig. 2 include a local area network (LAN) 180 and  
11 a wide area network (WAN) 182. Such networking environments are  
12 commonplace in offices, enterprise-wide computer networks, intranets, and the  
13 Internet.

14 When used in a LAN networking environment, computer 130 is connected  
15 to the local network 180 through a network interface or adapter 184. When used  
16 in a WAN networking environment, computer 130 typically includes a modem 186  
17 or other means for establishing communications over the wide area network 182,  
18 such as the Internet. The modem 186, which may be internal or external, is  
19 connected to the bus 136 via a serial port interface 156. In a networked  
20 environment, program modules depicted relative to the personal computer 130, or  
21 portions thereof, may be stored in the remote memory storage device. It will be  
22 appreciated that the network connections shown are exemplary and other means of  
23 establishing a communications link between the computers may be used.

24 Generally, the data processors of computer 130 are programmed by means  
25 of instructions stored at different times in the various computer-readable storage

1 media of the computer. Programs and operating systems are typically distributed,  
2 for example, on floppy disks or CD-ROMs. From there, they are installed or  
3 loaded into the secondary memory of a computer. At execution, they are loaded at  
4 least partially into the computer's primary electronic memory. The invention  
5 described herein includes these and other various types of computer-readable  
6 storage media when such media contain instructions or programs for implementing  
7 the steps described below in conjunction with a microprocessor or other data  
8 processor. The invention also includes the computer itself when programmed  
9 according to the methods and techniques described below.

10 For purposes of illustration, programs and other executable program  
11 components such as the operating system are illustrated herein as discrete blocks,  
12 although it is recognized that such programs and components reside at various  
13 times in different storage components of the computer, and are executed by the  
14 data processor(s) of the computer.

### 15 **Email Server System Architecture**

16  
17 Fig. 4 shows an exemplary email server system 34 in accordance with one  
18 embodiment of the invention. System 34 includes one or more email servers 36  
19 and a recipient storage location 38. Server 36 includes an email filter or filter  
20 processor 40 having a heuristic library 42 and a storage location 44 that is  
21 managed by email server 36. Although email server system 34 is shown as an  
22 integral unit, it is to be understood that the various constituent parts thereof can be  
23 separately implemented and associated with one another. Recipient storage  
24 location 38 includes a plurality of dedicated storage locations for each of the users  
25 or recipients, with exemplary locations being shown at 46, 48 and 50. Bulk email

1 messages are received at the email server location and are typically addressed to a  
2 plurality of recipients. Server 36 filters various email messages by applying one  
3 or more heuristics that are defined in heuristic library 42 to an incoming email  
4 message. The heuristics enable the filter to determine whether an email message  
5 likely constitutes an unwanted email message. One of the goals of some  
6 embodiments of the present invention is to ascertain whether an email message is  
7 unwanted without having to consider the message that is conveyed by the text of  
8 the email message. Accordingly, some of the heuristics are directed to looking at  
9 aspects of an email message that are not necessarily related to the content of the  
10 message itself. Thus, some heuristics consider the number of recipients to which a  
11 particular email message is addressed and the overall size of the email message. If  
12 the email message likely constitutes an unwanted email message, it is redirected to  
13 a first location such as storage location 44, rather than being placed in one or more  
14 of the dedicated storage locations 46, 48 and 50 for the addressed recipients. This  
15 constitutes but one way of ensuring that the server does not make as many copies  
16 of the email message as there are specified recipient addresses. Email messages  
17 that are found not likely to constitute unwanted email messages are delivered to  
18 the individual respective dedicated storage locations 46, 48 and 50 and can be  
19 provided to the recipients in due course.

20 In a preferred embodiment, only a single copy of the email message is  
21 maintained at storage location 44. Other copies can be made if a particular  
22 recipient has requested to receive email messages from a particular sender, as will  
23 become apparent below. This avoids having to reproduce the email message for  
24 each and every addressed recipient and store the email messages at multiple  
25 locations throughout the server system. Since many unwanted email messages are

1 bulk in nature (i.e. addressed to many intended recipients) storage location 44 can  
2 also be considered as a bulk email folder into which bulk email messages can be  
3 first placed.

4 Fig. 5 shows the Fig. 4 system after an email message has been received  
5 and determined to constitute an unwanted bulk email message or spam. The spam  
6 message is stored at storage location 44. Server 36 then notifies each of the  
7 intended recipients or specified addressees that an email has been received for  
8 them. One way of sending notification to the recipients is to place a pointer at a  
9 second location that is dedicated to each recipient, e.g. an email folder of each  
10 recipient. Then, when the recipient logs in to check their email, the pointer will  
11 allow them to access and read the stored email message if they so desire. This is  
12 preferably done without making any copies of the email message, other than the  
13 one that is stored at storage location 44. The recipient is also free to request that  
14 the server make a copy of the email message and store the email message in a  
15 dedicated recipient-specific storage location. In the illustrated example, the third  
16 recipient has requested a copy of the spam message which is now stored in their  
17 own dedicated storage location. In this example, storage location 44 is shared  
18 among the intended recipients. However, the fact that it is shared is virtually  
19 transparent to the recipients. By using the pointer that is placed at the second  
20 location, each recipient can open the corresponding email message (in which case  
21 they can view the shared copy), delete the email message (in which case the  
22 pointer is deleted), or move the email message (in which case an actual copy of the  
23 email message is itself generated and stored in a location designated by the  
24 recipient).

Fig. 6 shows a decision diagram generally at 200 that describes decision-making that can take place in accordance with an embodiment of the invention. Step 202 determines whether an email message matches a pattern that is associated with spam or unwanted email messages. One way of defining patterns is through the use of heuristics that are discussed below in more detail. If the email message likely constitutes an unwanted email message, then step 204 delivers one copy of the email message to a central location such as location 44. Preferably, the central location is one that can be shared by the intended recipients to read the email thereby eliminating the need to reproduce the email system wide for all of the intended recipients. Step 206 notifies the intended recipients that an email message has been received. The recipients are then free to access the email message at the shared location and request that they receive their own copy of the email message. If step 202 determines that an email message is not likely to be unwanted, then step 208 delivers the email message to a recipient location, such as locations 46, 48 and 50 in Fig. 5.

### Heuristics

One of the advantages of the present invention is the robust collection of heuristics that can be used by email server 36 to screen for unwanted email. Preferably, the heuristics are built upon the principle that unwanted email or spam typically exhibits a pattern when it is delivered. Many times this pattern is independent of the message that is conveyed by any of the content of a particular message. For example, one need not necessarily read the content of an unsolicited email describing adult web sites if it can be ascertained from other aspects of the message that it is likely to constitute unwanted email. For example, unwanted



email is typically addressed to a large number of specified recipient addresses. These addresses may not appear in the "To:" field, but rather will appear in the "BC" (blind copy) field, as in Fig. 1. Many times, a number of these addresses will be invalid as a result of being computer generated to cover a large number of address permutations. Additionally, some unwanted email messages might be very large in size. By recognizing these aspects of an email message, heuristics are designed that consider factors unrelated to a message's content. Content-based filtering can, however, still be used in connection with one or more of the embodiments of the invention. Hence, determinations concerning whether an email message is likely or not to constitute spam can be made, in some embodiments, without accessing any content of the sender's address field, the subject field, or the message field.

As a simple example only, nine heuristics are set forth in Table 1 below. These heuristics are not intended to limit the invention in any way. Rather, they are only given to illustrate certain approaches that can be taken.

**Table 1**

Heuristic	Heuristic Description
1	Is the email message addressed to more than <insert number> recipients?
2	Is the email message addressed to more than <insert number> percent of invalid addresses?
3	Is the email message larger than <insert number> bytes?
4	Is the email message indirectly addressed to more than <insert number> recipients?
5	Is the email message delivered after 11:30 P.M local time?
6	Heuristic 5 and any of Heuristics 1, 2, 3, or 4.
7	Heuristics 1 and 2.

8	Heuristics 1 or 2.
9	Heuristics 1 and 3.

Heuristic 1 determines whether a particular email message is addressed to a definable number of recipients. This recognizes a pattern that certain email messages that are unwanted are often addressed to a large number of recipients. The heuristic includes a parameter that is indicated by the "<insert number>" field. This permits the heuristic to be adjusted to accommodate different delivery patterns. Heuristic 2 determines whether a certain percentage of the specified addresses are invalid. This recognizes a pattern that often times an unwanted email message will be addressed to a large number of invalid accounts. The heuristic also includes a parameter that is indicated by the "<insert number>" field that permits the heuristic to be adjusted. Heuristic 3 determines whether an email message is larger than a definable size and includes a parameter that is indicated by the "<insert number>" field. This permits the heuristic to be adjusted to accommodate different delivery patterns. This heuristic recognizes a pattern that certain unwanted emails may have size characteristics that are distinguishable over ordinary email messages. Heuristic 4 determines whether an email message is indirectly addressed to a certain number of recipients and includes a parameter that is indicated by the "<insert number>" field. This permits the heuristic to be adjusted to accommodate different delivery patterns. This heuristic recognizes a pattern that unwanted email messages may have a large number of recipients "blind copied". An email message can be considered as indirectly addressed to a recipient if the recipient's address is not specified in the "TO" field, i.e. it appears either in the "CC" or "BC" fields. Heuristic 5 recognizes a pattern that certain

unwanted emails might typically be delivered after certain times in the evening. The remaining heuristics constitute combinations of the heuristics mentioned above.

The heuristics constitute but one way of defining different profiles that can be used to assess whether a particular email message is likely to be unwanted. By virtue of the fact that different combinations of heuristics can be used, and certain parameters values within certain heuristics can be varied, a robust set of flexible, adaptable profiles can be built and maintained. In addition, the profiles can be quickly adapted, system-wide, to address subtle changes in the delivery patterns of the spam.

### Desirability Index

In one embodiment, the concept of a desirability index is used to assess email messages. Fig. 7 shows one such exemplary index at 300. The idea behind the desirability index is that index values, here 1-7, are assigned to various degrees of desirability that an email message can have. The degrees of desirability range from a low desirability value of 1 to a high desirability value of 7. The index values are associated with a plurality of parameters having parameter values. For exemplary purposes only, Table 2 sets forth the index values that are cross-referenced against some example parameters.

**Table 2**

Index Values	Number of specified recipient addresses	Percentage of invalid specified recipient addresses	Larger than X bytes	Delivery time
1	>1000	>20%	>X	Between 11:30 P.M and 3:30 A.M.
2	$0 < y \leq 200$	>10%	>X	Between 10:00 P.M. and 12:00 P.M.

3	$0 < y \leq 150$	5-15%	$>X$	Daytime
4	$0 < y \leq 100$	5-10%	$<X$	Daytime
5	$\leq 30$	0-10%	$<X$	Daytime
6	$\leq 20$	0-5%	$<X$	Daytime
7	$\leq 20$	0-3%	$<X$	Daytime

The parameters in this example include: the number of specified recipient addresses, the percentage of invalid specified recipient addresses, a size parameter, and a delivery time parameter. The parameters each have values that correspond to the various index values. Some of the parameters do not depend on any message conveyed by any content of an email message. The parameter values are preferably adjustable so that different patterns of delivery can be examined.

Fig. 8 shows a user interface 302 that can be used in connection with desirability index 300. The user interface 302 is established so that a user, client, or recipient can adjust either or both of the individual parameter values or the index values. If the user adjusts a parameter value, then the index value associated with a certain degree of desirability is made either more or less restrictive. If the user adjusts the index value, then the user changes the degree of desirability. The email server then uses the selected index value to assess and evaluate incoming email messages for the user.

For example, when an email message is received at the server location, a score can be calculated based upon one or more of the parameters. Any number or combination of parameters can be used. In addition, parameters other than those specifically shown can be used. The score is then compared with an index value that is selected by a user or recipient. In this manner, the user-selected index value represents a threshold value. The index or threshold value defines a likelihood that a particular email message will constitute an unwanted email message. If an email message's score exceeds the threshold value (here, in the negative

1 direction), then the email message likely constitutes one that a user or recipient  
2 does not want. If this is the case, the server can then place a copy of the email  
3 message at storage location 44 (Fig. 5) and send notifications to the intended  
4 recipients.

### 6 **Address Screening of Bulk Mail**

7 Some bulk email messages, by their very nature, are desirable to some  
8 users. By simply screening the bulk email messages as described above, it is  
9 possible that some users might not see the bulk email messages. This is especially  
10 so if the email messages at the single, shared location are only maintained for a  
11 short determinable period of time. To address this situation, embodiments of the  
12 invention provide additional address screening for bulk email messages. Address  
13 screening permits a user or recipient to receive specified bulk email messages  
14 without having to read the email messages from the single, shared location. The  
15 user or recipient can specify a list of approved senders. This provides an  
16 advantageous way for a user to receive bulk email messages that they do not want  
17 to be filtered. For example, Microsoft may send bulk email messages that  
18 describe various software upgrades to its users. A user who wishes to receive  
19 these bulk email messages can simply add "microsoft.com" as a domain name  
20 from which email messages will always be accepted. In addition, address  
21 screening also permits users to screen bulk email messages based upon whether  
22 they are directly addressed in the email message, i.e. their address appears in the  
23 "TO" field and not in the "CC" or "BC" fields. This permits a user to screen  
24 potential bulk email messages by looking for email messages in which they are  
25 blind copied. Combining these two address screening techniques sets up a

1 powerful screening mechanism that allows only those bulk email messages that  
2 meet the specified criteria to be placed into a user-dedicated storage location. It  
3 should be apparent that as to other users who have not specifically placed a sender  
4 in their list of approved senders, the email message will be placed in the single,  
5 shared location and subsequent notifications will be sent out.

6 Fig. 9 shows a flow diagram at 400 that describes processing in accordance  
7 with one address screening embodiment. The server receives an email message at  
8 step 402 and determines it to be a bulk email message. Exemplary ways of  
9 determining whether an email message is a bulk message are described above and  
10 include determining the number of users or recipients to which the email message  
11 is addressed. The server then determines whether the bulk email message is  
12 addressed directly to a recipient at step 404. If a recipient's address appears in the  
13 "CC" or the "BC" field, it is not directly addressed to a recipient and is sent to the  
14 bulk email folder at step 408 and notifications are sent at step 410. If the email  
15 message is directly addressed to a recipient, step 406 determines whether the  
16 sender is on the recipient's list of approved senders. If the sender is not on the  
17 approved list, then the email message is sent to the bulk email folder at step 408  
18 and notifications are sent at step 410. If the sender is on the recipient's list of  
19 approved senders, then the email message is delivered or placed in a dedicated  
20 recipient location at step 412, such as the user storage locations mentioned above.

### 21 22 **Content Screening**

23 Other embodiments of the invention recognize the fact that bulk email  
24 messages or spam often contains text that is identical or very similar to other bulk  
25 email messages or spam. This is the case, for example, when the same email

1 messages are sent at different times, or the same or similar email messages are  
2 sitting in a queue awaiting delivery. For example, spammers may target some  
3 recipients on one day, and then target other recipients on another day with the  
4 same email message. If, for some reason, the spam escapes filtering when it is  
5 first sent, then it may be possible to pick it up on the second day if it is similar in  
6 content. Thus, a profile can be developed of unwanted email messages based  
7 upon whether the email messages are similar in content with other email  
8 messages. Email messages can be similar in content if they are identical or if they  
9 contain a definable amount of textual similarities. The email server then looks for  
10 email messages that meet the established profile. If the profile is met, then  
11 processing can take place as described above.

12 Application of the profile can take place by conducting simple text searches  
13 of the email messages that are received to ascertain whether any of their text  
14 matches text of any other email messages such as those that have been found to be  
15 spam. Alternately, different text-matching algorithms can be employed such as  
16 fuzzy text-matching algorithms that impart a degree of intelligence to the email  
17 server.

### 18 19 **Hotmail Architecture**

20 Preferred embodiments are implemented in conjunction with Microsoft's  
21 Hotmail service. Fig. 10 is a diagram that shows general architectural features of  
22 the Hotmail system generally at 500. A Hotmail "cloud" 502 encapsulates all of  
23 the Hotmail functionality so that everything a user or client sees on their screen is  
24 generated inside the Hotmail cloud. Hotmail cloud 502 includes an array of web  
25 servers 504. When a user logs in, they communicate with one of the servers of the

1 array. The web servers are configured to serve web pages and do not contain any  
2 user data. The web servers can either pull HTML files off a storage disk or run a  
3 program to generate an appropriate HTML file. The file is then provided to a user  
4 browser executing on a user machine that requested the HTML file and is  
5 assembled by the browser at the user machine.

6 Hotmail cloud 502 includes one or more user database servers 506. All  
7 user or recipient data resides on the user database servers. This includes, for each  
8 account, all email messages, contact lists, personal preferences, passwords, and all  
9 other items typically associated with an email account. In practice, the user  
10 database servers are implemented by SUN Ultra Enterprise 4500-class servers.  
11 Each server stores from between 750,000 to 2,000,000 user accounts.

12 A database server 508 is provided and is an internal database server. Server  
13 508 includes a list of all Hotmail users in memory, as well as the location of their  
14 user data on database servers 506. When a user contacts the Hotmail cloud 502, a  
15 web server of the web server array 504 contacts database server 508 to ascertain  
16 the location of the user's data on one of the user databases 506. The database  
17 server 508 returns the location to the web server which then can either assist a user  
18 in reading their email messages or assist a user in sending email messages.

19 When an email message is read by a user, the list of email messages are  
20 pulled by a web server of web server array 504. An appropriate web page is  
21 generated to appear as an email inbox. Links are embedded in the web page for  
22 the particular email messages. The web page is then sent to the user and  
23 assembled by the user's browser. The links retrieve the particular email messages  
24 for a user.  
25



1 When email is sent, a user clicks on an appropriate composition page which  
2 brings up a web page that looks like an email page. The user types a message and  
3 clicks send. The email message is packaged as an *http* web request that is received  
4 by a server of the server array 504. The web server then contacts database server  
5 508 to ascertain the location of the intended recipient. If the recipient exists, then  
6 their location is returned to the web server which then deposits the email message  
7 in the appropriate account. This process is utilized for the users that are within the  
8 Hotmail cloud 502. That is, these users are subscribers to the Hotmail email  
9 service. Email messages can, however, be received into the Hotmail cloud from  
10 outside of the cloud, e.g. from the users that are depicted outside of the cloud in  
11 Fig. 10.

12 Hotmail cloud 502 also includes an array of SMTP mail servers 510 that  
13 perform essentially the same as server array 504. That is, when an email message  
14 is received from outside of the cloud, a server of array 510 contacts database  
15 server 508 to ascertain a recipient location among user databases 506, and then  
16 deposits the email message at one or more of the appropriate locations. The  
17 SMTP servers are completely open to the network through which the email  
18 messages come. The servers are unable to authenticate whether the sender of an  
19 email message is an actual sender or not. Additionally, the SMTP servers 510 are  
20 unable to authenticate the server that connects with it to deliver the email message.  
21 Because of this, spam can easily enter the Hotmail cloud 502.

22 When spam arrives, the server array (either of arrays 504 and 510) makes  
23 as many copies of the spam as there are valid recipients, and places each copy in a  
24 dedicated user storage location provided by user database 506. With millions of  
25

1 Hotmail users, it is easy to see how spam can be promulgated throughout the  
2 Hotmail system and consume valuable and expensive memory.

3 In preferred embodiments, server arrays 504 and 510 are configured to  
4 screen email message based upon a set of heuristics that determine whether an  
5 email message is likely to constitute an unwanted email message. Alternately, a  
6 dedicated server that is linked with each of these server arrays can perform the  
7 email screening functions. Exemplary heuristics are discussed above. If an email  
8 message is found to likely constitute an unwanted email message, a single copy is  
9 placed in a storage location that is not a dedicated user storage location. The  
10 server then notifies all of the valid specified recipients that an email message for  
11 them has been received. This can take place as discussed above.

### 12 13 **Conclusion**

14 Various embodiments of the invention address two critical problems that  
15 current email service providers face. First, there is the problem of maintaining  
16 high levels of customer service when email server systems are inundated with  
17 spam. Second, there is the problem of reducing the system-wide impact that spam  
18 has on the email delivery system. Current embodiments are directed to  
19 determining whether an email message is an unwanted bulk email message  
20 without necessarily considering the message that is conveyed by any portion of the  
21 email message. Through analyses of patterns of delivery of these email messages,  
22 profiles are built that allow an email server to ascertain whether there is a  
23 likelihood that any one particular email message constitutes an unwanted email  
24 message. If an email message is determined to likely constitute an unwanted  
25 email message, then memory-saving measures are implemented. In preferred



1 **CLAIMS**

2       1.     An email filtering method comprising:  
3       defining at least one heuristic that determines whether an incoming email  
4       message likely constitutes unsolicited commercial email by considering an  
5       established pattern that such unsolicited commercial email typically exhibits when  
6       it is sent;

7       applying said at least one heuristic to at least one email message; and  
8       redirecting said at least one email message if application of said at least one  
9       heuristic indicates that said at least one email message likely constitutes  
10      unsolicited commercial email.

11  
12       2.     The email filtering method of claim 1, wherein said redirecting  
13      comprises placing a copy of the email message at a single location from which it  
14      can be accessed by more than one intended recipient of the email message.

15  
16       3.     The email filtering method of claim 1, wherein said defining  
17      comprises defining a plurality of heuristics that are independent of the message  
18      conveyed by any of the content contained in an email message.

19  
20       4.     The email filtering method of claim 1, wherein said at least one  
21      heuristic has at least one parameter that can be adjusted, and further comprising  
22      adjusting said at least one parameter to vary the pattern that is considered.

004020"256450

1           5.    The email filtering method of claim 1, wherein said at least one  
2 heuristic considers a pattern associated with the number of specified recipient  
3 addresses of the email message.

4  
5           6.    The email filtering method of claim 5, wherein the pattern is  
6 associated with the number of invalid specified recipient addresses.

7  
8           7.    The email filtering method of claim 1, wherein said at least one  
9 heuristic considers a pattern associated with the size of an email message.

10  
11           8.    The email filtering method of claim 1, wherein said at least one  
12 heuristic considers patterns associated with the number of specified recipient  
13 addresses of the email message and the size of the email message.

14  
15           9.    The email filtering method of claim 1 further comprising after said  
16 redirecting, notifying at least one intended recipient that an email message  
17 intended for them has been redirected.

18  
19           10.   The email filtering method of claim 1, wherein said redirecting  
20 comprising redirecting said at least one email message to a location that can be  
21 shared by a plurality of intended recipients for reading said email message, and  
22 further comprising after said redirecting, notifying intended recipients of the email  
23 message that an email message intended for them has been redirected to said  
24 location.

1           **11.**    The email filtering method of claim 10, wherein said redirecting  
2 comprises storing only one copy of the email message.

3  
4           **12.**    An email filtering method comprising:  
5           receiving an email message at an email server that maintains inboxes for  
6 individual recipients, wherein the email message is addressed to a plurality of  
7 recipients;

8           calculating a score for the email message at the server location based upon  
9 at least one of (a) the size of the email message, and (b) the number of specified  
10 recipient addresses;

11           comparing the score with a threshold value that defines a likelihood of  
12 whether an email message constitutes an unwanted email message;

13           responsive to the email message exceeding the threshold value, placing a  
14 copy of the email message at a first location other than any of the intended  
15 recipients' inboxes; and

16           sending a notification to the intended recipients that a copy of an email  
17 message that was intended for them has been placed at the first location.

18  
19           **13.**    The email filtering method of claim 12, wherein the threshold value  
20 is determined independent of the message conveyed by any of the text that is  
21 contained in any part of the email message.

1           **14.**    The email filtering method of claim 12, wherein the score is based  
2 upon both the size of the email message and the number of specified recipient  
3 addresses.

4  
5           **15.**    The email filtering method of claim 12, wherein said first location is  
6 a storage location that is managed by the email server.

7  
8           **16.**    The email filtering method of claim 12, wherein said threshold value  
9 is based upon the number of invalid specified recipient addresses.

10  
11          **17.**    The email filtering method of claim 12, wherein said sending of the  
12 notification comprises placing a pointer in an email folder of each recipient of the  
13 email message.

14  
15          **18.**    The email filtering method of claim 12 further comprising  
16 responsive to a request from a recipient, making a recipient copy of the email  
17 message and placing the recipient copy at a dedicated recipient storage location.

18  
19          **19.**    A computer program stored on one or more computer readable  
20 media for processing email, the program comprising the following steps:

21               receiving an email message at a server location, the email message being  
22 addressed to a plurality of recipients;

23               placing only one copy of the email message at a first storage location that is  
24 not a dedicated storage location for just one of the intended recipients; and  
25

1 notifying each of the intended recipients that an email message intended for  
2 them has been placed at the first location.

3  
4 **20.** The steps of claim 19, wherein the first storage location is a storage  
5 location that is managed by a server associated with the server location.

6  
7 **21.** The steps of claim 19, wherein the first storage location is a storage  
8 location that is managed by a server associated with the server location, and is  
9 accessible to any of the intended recipients.

10  
11 **22.** The steps of claim 19, wherein said notifying comprises creating a  
12 pointer to the first location, and placing the pointer at a plurality of second  
13 locations each of which being dedicated to a different one of the intended  
14 recipients, wherein individual recipients can use the pointer to access the email  
15 message at the first storage location.

16  
17 **23.** The steps of claim 19 further comprising prior to said placing:  
18 defining a profile of unwanted email messages based upon at least one of:  
19 the size of an email message, the number of specified recipient addresses, and the  
20 number of invalid specified recipient addresses;

21 determining whether an email message meets the profile; and

22 wherein said placing and said notifying takes place only if the email  
23 message meets the profile.



1       **24.** A programmed email server that contains computer-readable  
2 instructions which, when executed by the email server, perform the following  
3 steps:

4           determining whether an email message that is received by the email server  
5 likely constitutes an unwanted email message; and

6           if the email message likely constitutes an unwanted email message:

7               storing a copy of the email message at a first storage location rather  
8 than individual storage locations that are dedicated to individual intended  
9 recipients of the email message; and

10           notifying intended recipients of the email message that an email  
11 message addressed to them has been received by the server.

12  
13       **25.** The steps of claim 24, wherein said determining takes place without  
14 considering the message conveyed by any content of the sender's address field, the  
15 subject field, or the message field.

16  
17       **26.** The steps of claim 24 further comprising enabling intended  
18 recipients, if they so desire, to read the email message at the first storage location.

19  
20       **27.** The steps of claim 26, wherein said enabling comprises doing so  
21 without making any copies of the copy of the email message at the first storage  
22 location.

004020" 25625460

1           **28.**     The steps of claim 26 further comprising receiving instructions from  
2 an intended recipient that a copy of the email message be made specifically for  
3 them, and responsive thereto, making a copy of the email message, and storing  
4 said copy at a recipient-specific location.

5  
6           **29.**     The steps of claim 24, wherein said determining takes place by  
7 considering the size of the email message.

8  
9           **30.**     The steps of claim 24, wherein said determining takes place by  
10 considering the number of specified recipient addresses of the email message.

11  
12           **31.**     The steps of claim 24, wherein said determining takes place by  
13 considering the number of invalid specified recipient addresses.

14  
15           **32.**     The steps of claim 24, wherein said determining takes place by  
16 defining a plurality of heuristics that establish a profile of unwanted email  
17 messages, wherein the profile considers factors that are independent of any  
18 message conveyed by an email message's content, and applying the plurality of  
19 heuristics to an email message.

20  
21           **33.**     The steps of claim 32, wherein the heuristics are adjustable.  
22  
23  
24  
25

1           **34.**     An email screening method comprising:  
2           developing a profile of unsolicited commercial email based upon the size of  
3           an email message and the number of specified recipient addresses of the email  
4           message;  
5           configuring a mail server that is responsible for storing and distributing  
6           email messages to a plurality of clients with a filter processor that is programmed  
7           to evaluate email messages that are received in light of the developed profile;  
8           evaluating email messages with the filter processor and determining  
9           whether the email messages fit the developed profile; and  
10          if an email message fits the developed profile, initiating a remedial measure  
11          that ensures that the mail server does not make as many copies of the email  
12          message as there are specified recipient addresses.

13  
14          **35.**     The email screening method of claim 34, wherein said remedial  
15          measure comprises storing one copy of the email message at a server storage  
16          location, instead of storing multiple copies of the email message for the specified  
17          recipient addresses.

18  
19          **36.**     The email screening method of claim 34, wherein said remedial  
20          measure comprises storing one copy of the email message at a server storage  
21          location, instead of storing multiple copies of the email message for the specified  
22          recipient addresses, and notifying intended recipients that an email message  
23          intended for them has been stored at the server storage location.

1           **37.**    The email screening method of claim 34, wherein said remedial  
2 measure comprises storing one copy of the email message at a server storage  
3 location, instead of storing multiple copies of the email message for the specified  
4 recipient addresses, and notifying intended recipients that an email message  
5 intended for them has been stored at the server storage location by placing a  
6 pointer in a designated email folder for the intended recipients.

7  
8           **38.**    The email screening method of claim 37 further comprising, for  
9 each recipient who so desires, reading the email message from the server storage  
10 location.

11  
12           **39.**    The email screening method of claim 37 further comprising, for  
13 each recipient who so desires, copying the email message from the server storage  
14 location to a recipient-location.

15  
16           **40.**    An email delivery method comprising:  
17           establishing a bulk email folder in which bulk email is to be stored;  
18           configuring an email server to receive email messages and deliver them  
19 either to multiple server storage locations that are dedicated to storing email  
20 messages for respective recipients or to a single, shared location that can be shared  
21 by a plurality of the recipients;  
22           receiving an email message;  
23           comparing an address for the sender of the email message with a recipient's  
24 list of approved senders; and  
25

1 delivering the email message to the single, shared location if: (a) the email  
2 message is not directly addressed to a recipient that is serviced by the server, and  
3 (b) the sender's address does not appear in the recipient's list of approved senders.  
4

5 **41.** The email delivery method of claim 40 further comprising  
6 maintaining the email message at the single, shared location only for a  
7 determinable amount of time.  
8

9 **42.** An email screening method comprising:  
10 developing a profile of unwanted email messages based upon whether an  
11 email message is similar in content to another email message;

12 configuring a mail server that is responsible for storing email messages for  
13 a plurality of clients with a filter processor that is programmed to evaluate email  
14 messages that are received in light of the developed profile;

15 evaluating email messages with the filter processor and determining  
16 whether the email message fits the developed profile; and

17 if the email message fits the developed profile, placing a copy of the email  
18 message in a first location and, rather than placing multiple copies of the email  
19 message in multiple dedicated client storage locations, notifying the multiple  
20 clients that an email message addressed to them has been received so that the  
21 clients can read the email message if they so desire.  
22  
23  
24  
25

1           **43.**    An email screening method comprising:

2           defining an index having values that are assigned to various degrees of  
3           desirability that an email message can have, wherein the degrees of desirability  
4           extend from a low degree of desirability to a high degree of desirability;

5           associating a plurality of parameters having parameter values with the  
6           various degrees of desirability, wherein at least some of the parameters do not  
7           depend on any message that is conveyed by any content of an email message; and

8           establishing a user interface through which a user can adjust either (a)  
9           individual parameter values that, in turn, establish a degree of desirability, or (b)  
10          index values that themselves establish a degree of desirability that email messages  
11          must have in order to be saved to dedicated user storage locations; and

12          evaluating incoming email messages against the index value that is defined  
13          by the user.

14  
15          **44.**    The email screening method of claim 43, wherein the parameter  
16          values are adjustable.

17  
18          **45.**    The email screening method of claim 43, wherein one of the  
19          parameters is associated with the number of specified recipient addresses.

20  
21          **46.**    The email screening method of claim 43, wherein one of the  
22          parameters is associated with a percentage of invalid specified recipient addresses.  
23  
24  
25

1           **47.**     The email screening method of claim 43, wherein one of the  
2 parameters is associated with the size of an email message.

3  
4           **48.**     An email server system comprising:  
5           a user storage database configured to store user information including email  
6 messages that are intended for individual users; and

7           a server configured to receive email messages that are intended for various  
8 users and store the email messages in dedicated user storage locations within the  
9 user storage database;

10          wherein the server is further configured to screen email messages based  
11 upon a set of heuristics that determine whether an email message likely constitutes  
12 an unwanted email message, the server further being configured to place a single  
13 copy of an email message in a storage location that is not a dedicated user storage  
14 location if it is determined by screening the email message that it likely constitutes  
15 an unwanted email message.

16  
17          **49.**     The email server system of claim 48, wherein the set of heuristics  
18 considers the size of an email message.

19  
20          **50.**     The email server system of claim 48, wherein the set of heuristics  
21 considers the number of specified user addresses that are specified by an email  
22 message.

004020" 21546460

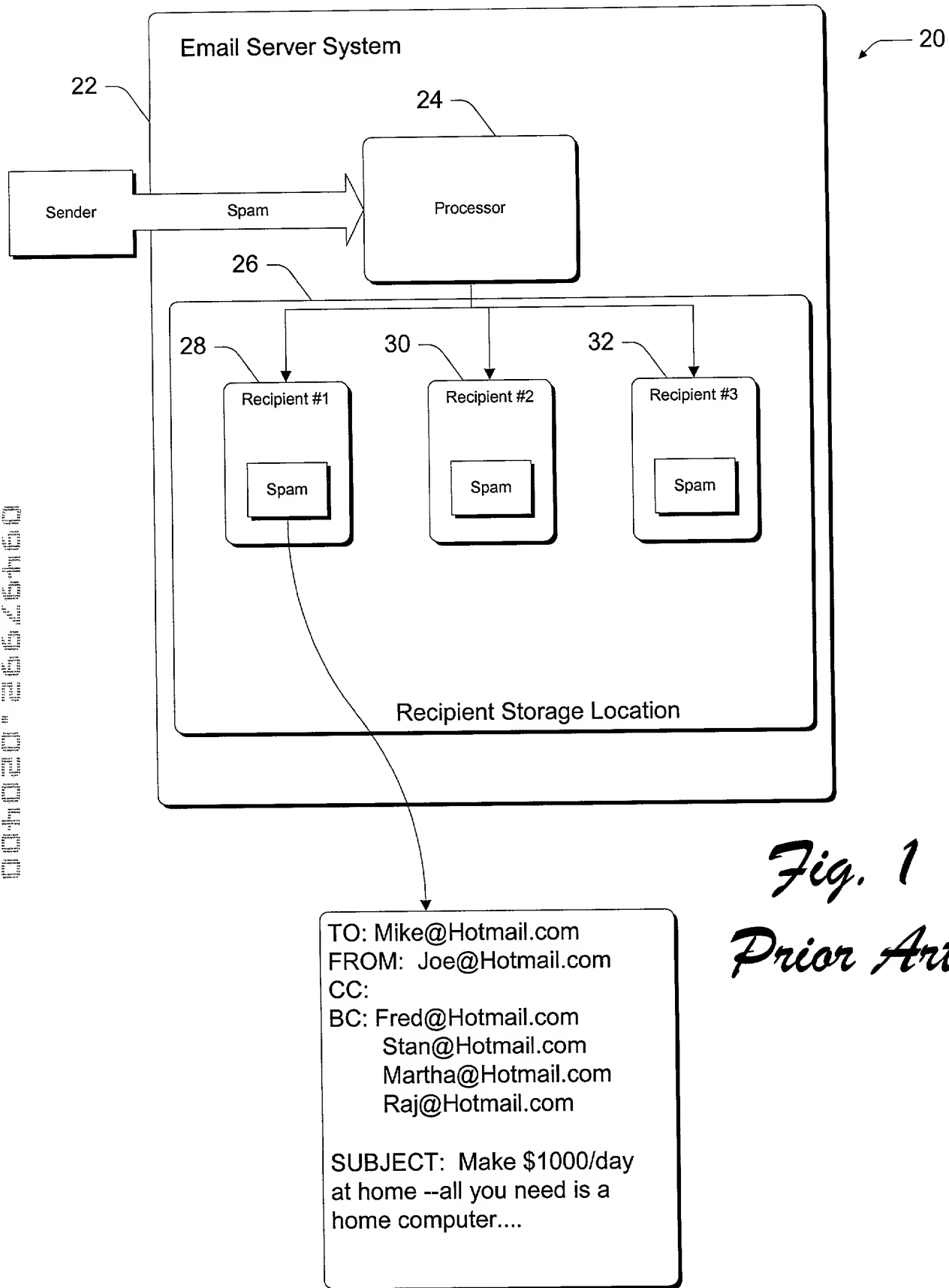
1           **51.**    The email server system of claim 48, wherein the set of heuristics  
2 considers the number of invalid specified user addresses that are specified by an  
3 email message.

4  
5           **52.**    The email server system of claim 48, wherein the server is further  
6 configured to place a pointer to the storage location in which the single copy of the  
7 email message is placed, in each dedicated user storage location that corresponds  
8 to a valid specified user address contained in the email message.



1 **ABSTRACT**

2 Various embodiments of the invention address two critical problems that  
3 current email service providers face. First, there is the problem of maintaining  
4 high levels of customer service when email server systems are inundated with  
5 spam. Second, there is the problem of reducing the system-wide impact that spam  
6 has on the email delivery system. Current embodiments are directed to  
7 determining whether an email message is an unwanted bulk email message  
8 without necessarily considering the message that is conveyed by any portion of the  
9 email message. Through analyses of patterns of delivery of these email messages,  
10 profiles are built that allow an email server to ascertain whether there is a  
11 likelihood that any one particular email message constitutes an unwanted email  
12 message. If an email message is determined to likely constitute an unwanted  
13 email message, then memory-saving measures are implemented. In preferred  
14 embodiments, one copy of the email message is saved at a central, shared location  
15 that can be accessed by each of the intended recipients. This avoids having to  
16 replicate the email message across the system for each of the recipients.  
17  
18  
19  
20  
21  
22  
23  
24  
25



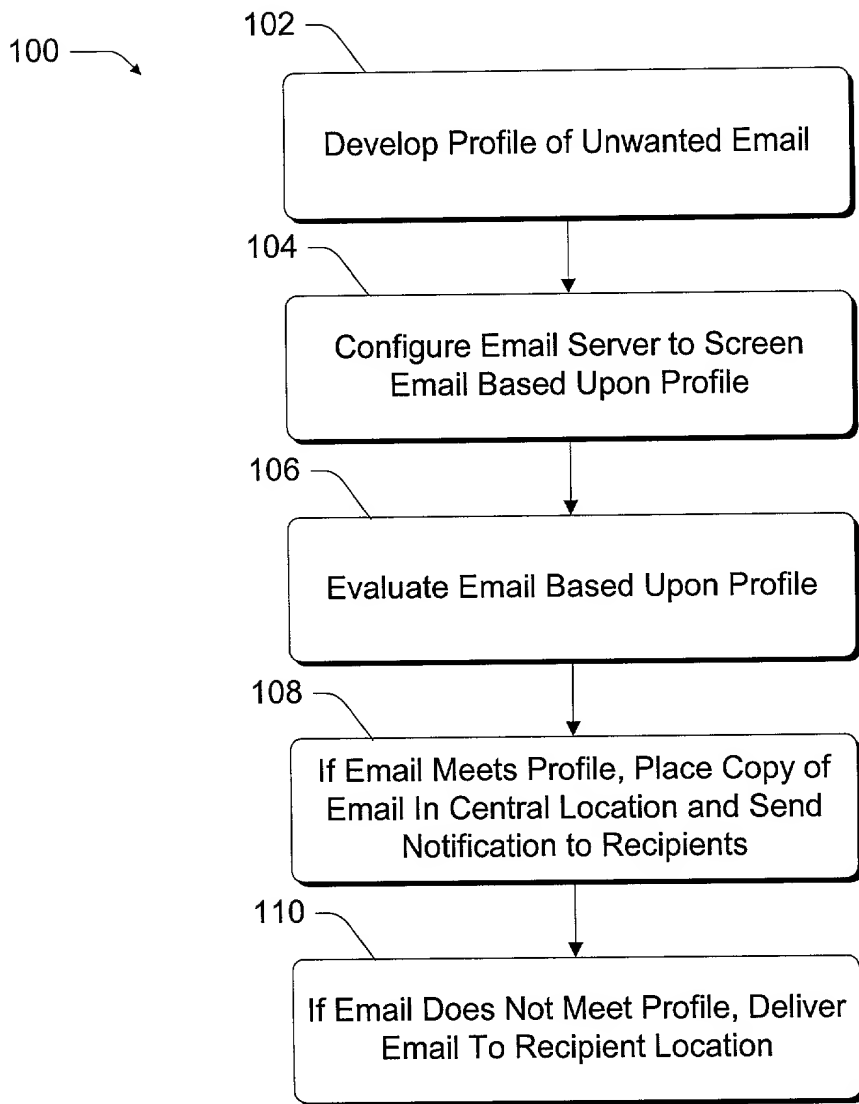
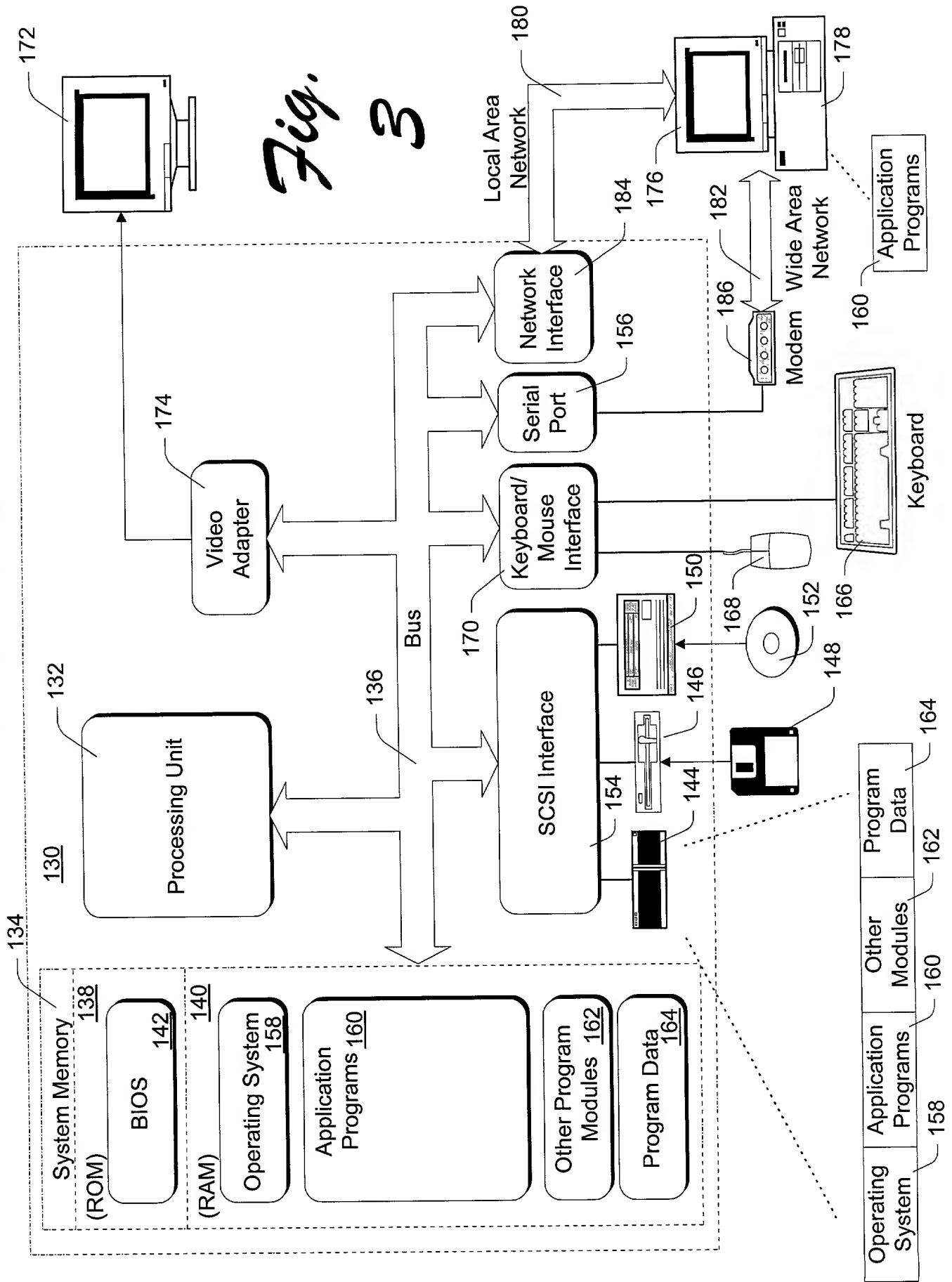
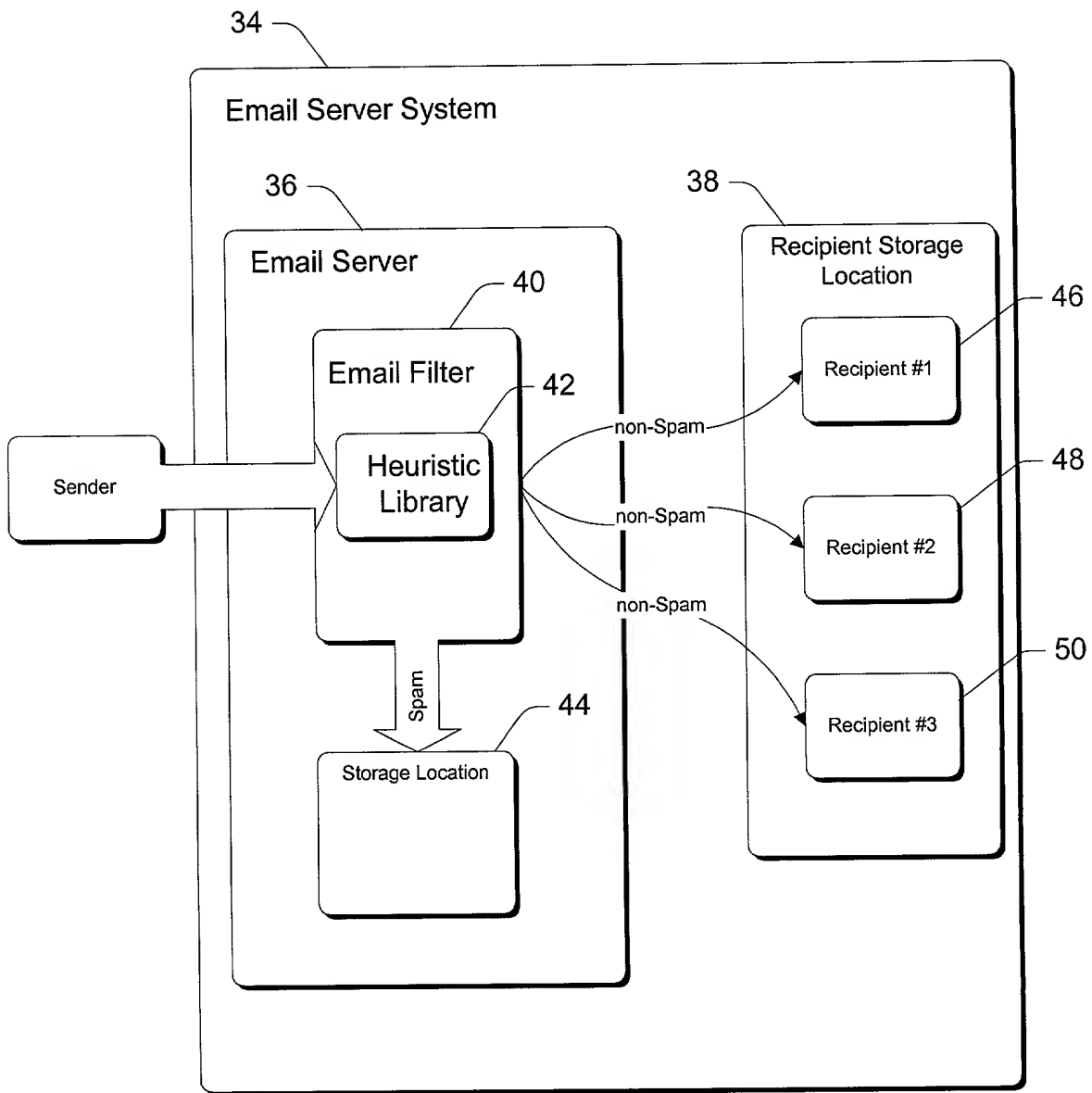
*Fig. 2*

Fig. 3



*Fig. 4*

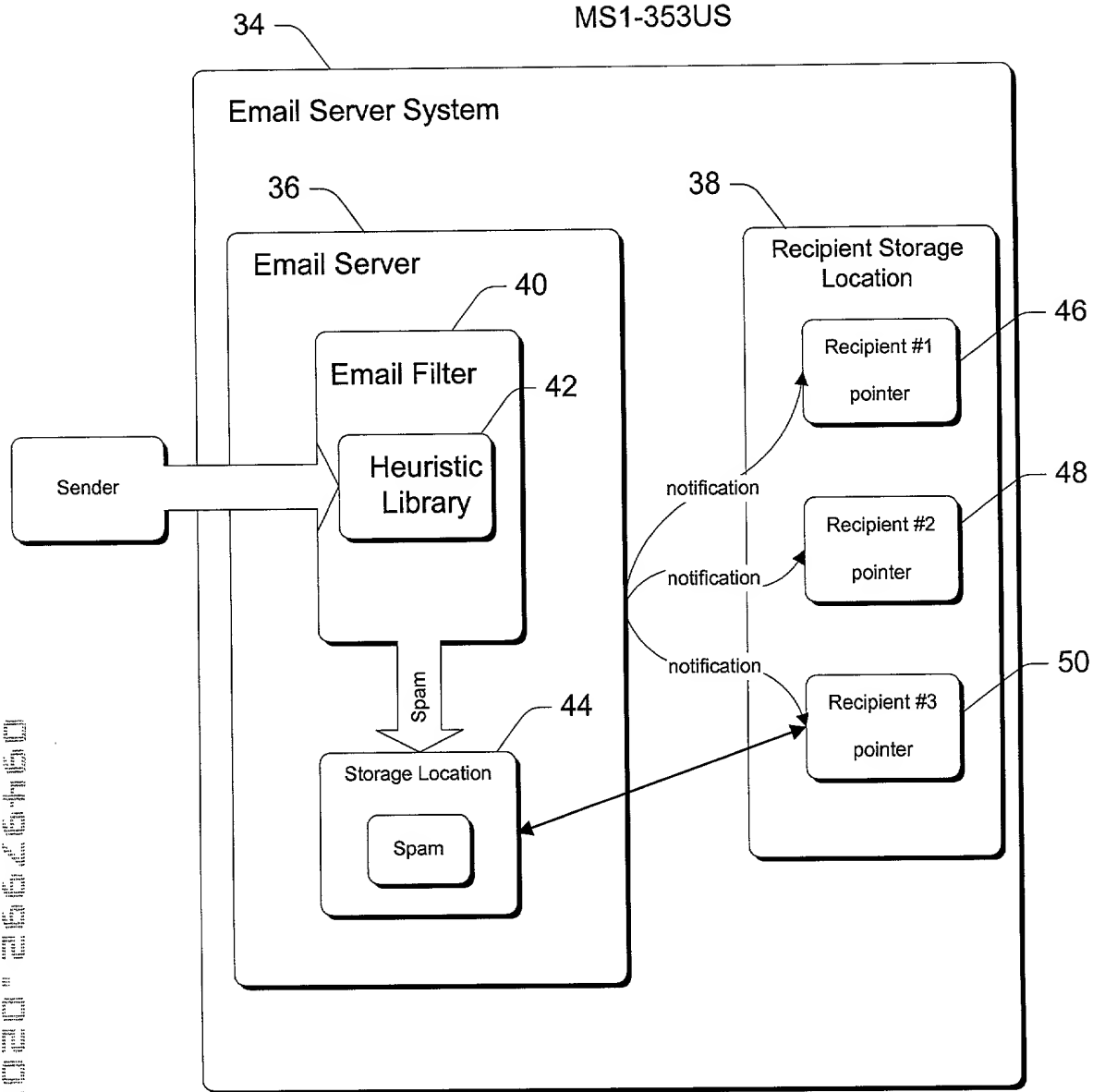


Fig. 5

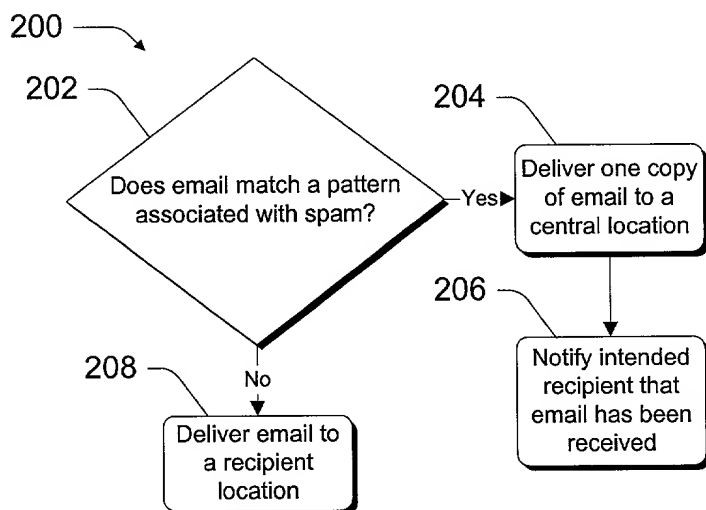
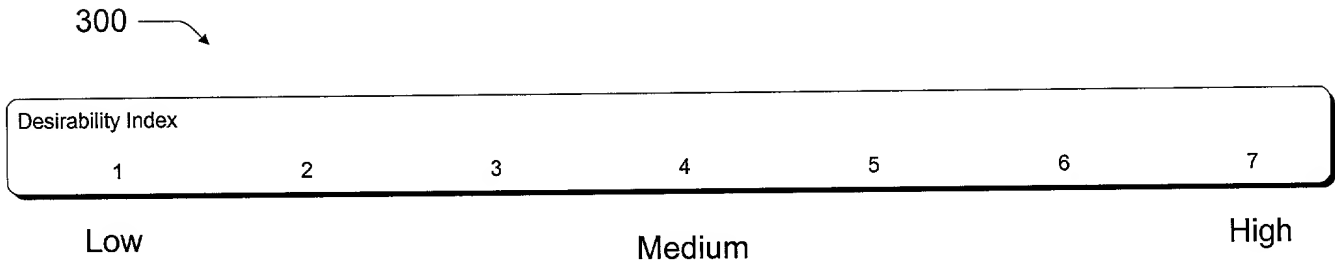
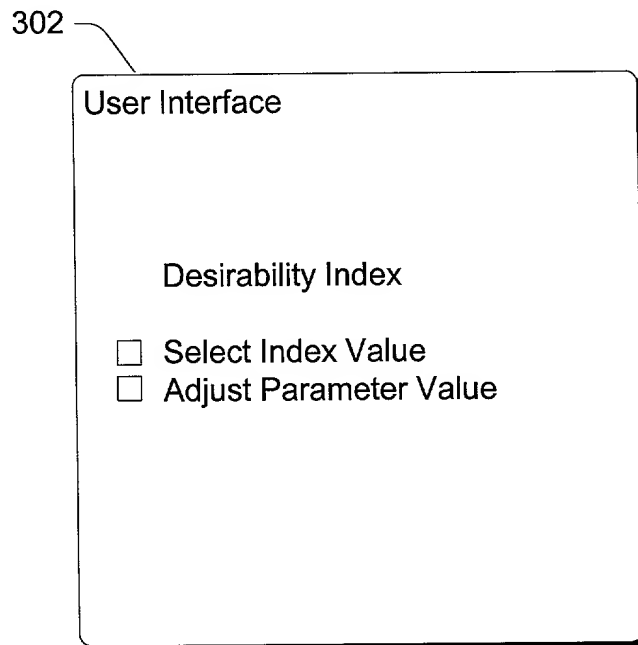


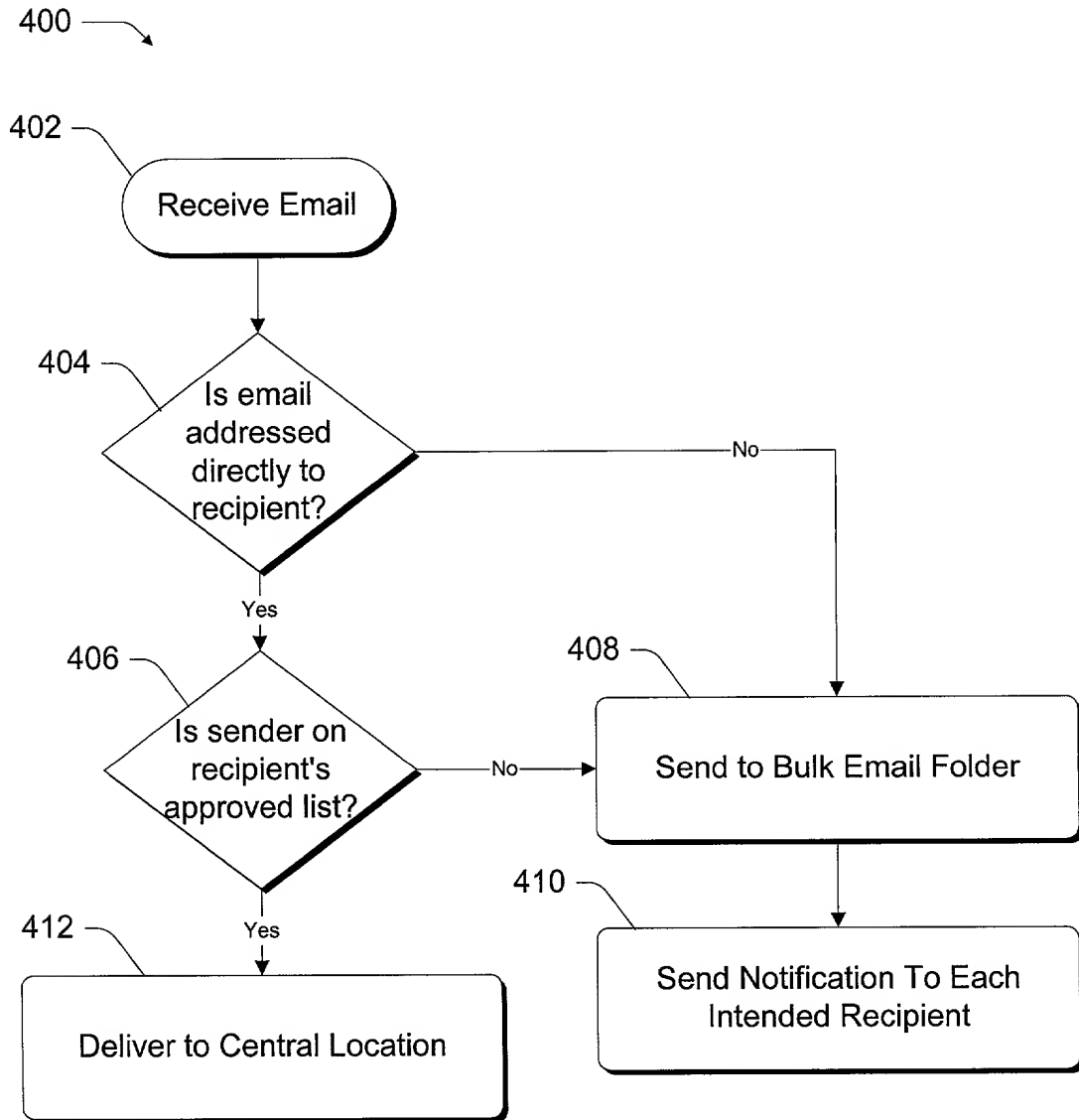
Fig. 6



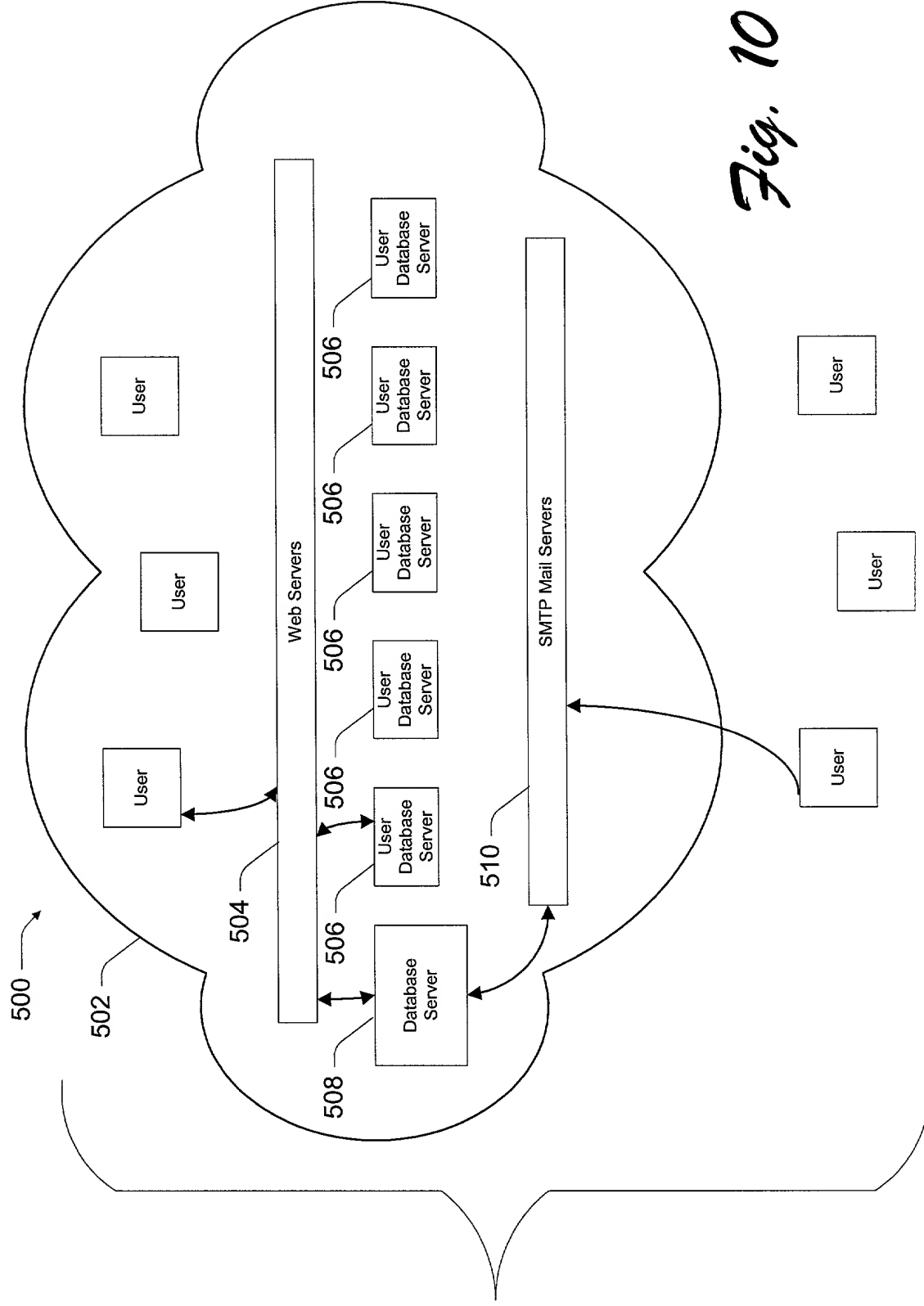
*Fig. 7*



*Fig. 8*

*Fig. 9*





IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventorship ..... Maller  
 Applicant ..... Microsoft Corporation  
 Attorney's Docket No. .... MS1-353US  
 Title: Email Filtering Methods and Systems

**DECLARATION FOR PATENT APPLICATION**

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled "Email Filtering Methods and Systems," the specification of which is attached hereto.

I have reviewed and understand the content of the above-identified specification, including the claims.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, § 1.56(a).

PRIOR FOREIGN APPLICATIONS: no applications for foreign patents or inventor's certificates have been filed prior to the date of execution of this declaration.

**Power of Attorney**

I appoint the following attorneys to prosecute this application and transact all future business in the Patent and Trademark Office connected with this application:  
 Lewis C. Lee, Reg. No. 34,656; Daniel L. Hayes, Reg. No. 34,618; Allan T.

Sponseller, Reg. 38,318; Steven R. Sponseller, Reg. No. 39,384; James R. Banowsky, Reg. No. 37,773; Lance R. Sadler, Reg. No. 38,605; Michael A. Proksch, Reg. No. 43,021; Thomas A. Jolly, Reg. No. 39,241; David A. Morasch, Reg. No. 42,905; Kasey C. Christie, Reg. No. 40,559; Katie E. Sako, Reg. No. 32,628 and Daniel D. Crouse, Reg. No. 32,022.

Send correspondence to: LEE & HAYES, PLLC, 421 W. Riverside Avenue, Suite 500, Spokane, Washington, 99201. Direct telephone calls to: Lance R. Sadler (509) 324-9256.

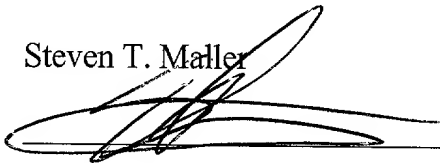
All statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statement may jeopardize the validity of the application or any patent issued therefrom.

\*\*\*\*\*

Full name of inventor:

Steven T. Maller

Inventor's Signature



Date: 1/25/2000

Residence:

Burlingame, CA

Citizenship:

USA

Post Office Address:

301 Chapin Lane  
Burlingame, CA 94010